Elementos de Criptografia

Curso de Licenciatura em Matemática Aplicada e Computação

Exame - 2ª Época 12 val.

Nota mínima 5 valores

Duração: 2 horas 30 minutos

Grupo I 1.0+1.0+1.0

1 Mostre, sem recorrer ao Teorema de Shannon, que a cifra de transposição permite segurança perfeita desde que a chave seja escolhida de forma uniforme. Explique porque é que o fluxo de chaves por blocos desta cifra não é perfeitamente seguro. Descreva um método para analisar este fluxo.

2 Considere um sistema criptográfico $\mathcal{S} = \langle X, X, C, e, d\rangle$ onde C possui uma estrutura de monóide $(C, id, \bullet)$ tal que $e_{id} = id_X$ e $e_{c\bullet c'} = e_c \circ e_{c'}$. Mostre que $\mathcal{S}$ é idempotente. Usando este resultado mostre que as cifras de transposição e de Hill são idempotentes.

3 Construa o circuito de encriptação e decifração da cifra de blocos DES. Recorde que este sistema tem input x e output y em $\mathbb{Z}_2^{64}$ e chave em $C \in \mathbb{Z}_2^{56}$. A descrição do algoritmo de encriptação é a seguinte:

1. Aplicar uma permutação inicial $IP(x) = [L_0, R_0]$ onde L_0 são os primeiros 32 bits de $IP(x)$ e R_0 os últimos 32 bits de $IP(x)$.
2. for i=1 to 16 with step 1 do
   (a) $L_i = R_{i-1}$
   (b) $R_i = L_{i-1} \oplus f(R_{i-1}, C_i)$ onde f corresponde a uma função predefinida e $\{C_i\}_{1\leq i\leq 16}$ é um fluxo finito de chaves em $\mathbb{Z}_2^{48}$ obtido de C.
3. Aplicar $IP^{-1}(R_{16}L_{16})$ e obter desta forma a encriptação de x.

Explique sucintamente os modos CFB, CBC e OFB do DES.

Grupo II 2.5+2.5

1. Explique o esquema de assinatura de ElGammal. Mostre como pode atacar este sistema se $p-1$ se factorizar em potências de primos pequenos. Indique como pode estender o ataque anterior para analisar o sistema criptográfico de ElGamal generalizado.

2. Seja $n = pq$ onde p e q são primos distintos, tais que $p,\ q = 3 \mod 4$. Mostre que se $a \in RQ(n)$ então a tem quatro raízes quadradas, mostre também que apenas uma destas raízes está em $RQ(n)$.

Considere a seguinte função $f : RQ(n) \to RQ(n)$ tal que $f(x) = x^2 \mod n$. Mostre que, dados p e q, pode computar $f^{-1} : RQ(n) \to RQ(n)$ em tempo polinomial, indicando a complexidade computacional do seu algoritmo.

Considere a seguinte linguagem $L \subseteq RQ(n) \times \mathbb{Z}_n$ tal que $L(f(x), y) = 1$ sse $x < y$. Mostre que se $L \in \mathbf{P}$ então é possível analisar com um algoritmo de tempo polinomial de Las Vegas o RSA e o sistema criptográfico de Rabin.

Grupo III 1.5+2.5

1. Construa um esquema para distribuir uma chave de um sistema de mísseis. Esta chave deve ser distribuída por três generais e três políticos de tal forma que sejam necessários três indivíduos para lançar o míssil. Entre estes indivíduos deve estar sempre presente um general e um político.

2. Descreva o protocolo de identificação de Schnorr. Mostre que a seguinte variante não é segura: A Alice possui uma chave secreta $n = pq$, onde $p, q = 3 \mod 4$. Os valores de n e $ID(A)$ são assinados pela AC e guardados no certificado $C(A)$ da Alice. Quando a Alice se quer identificar ao Bruno começa por enviar-lhe o seu certificado $C(A)$. De seguida, o Bruno apresenta à Alice um elemento $x \in RQ(n)$ escolhido uniformemente. Quando a Alice recebe x, calcula $y = \sqrt{x} \mod n$ e envia y ao Bruno. O Bruno identifica a Alice sse $y^2 = x \mod n$. Indique, justificado, se esta variante é adequada.